O I P E IAP41
APR 2 3 2007
PATENT & TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	J. Rosenberger	Attorney Docket No.: WIMET121663
Application No.:	10/669,124	Art Unit: 2131 / Confirmation No: 2882
Filed:	September 23, 2003	Examiner: C.A. Revak
Title:	SYSTEM AND METHOD FOR WIRELESS LOCAL AREA NETWORK MONITORING AND INTRUSION DETECTION	

DECLARATION UNDER 37 C.F.R. § 1.131

Seattle, Washington 98101

April 16, 2007

TO THE COMMISSIONER FOR PATENTS:

I, Jim Flanagan, declare:

1. I am Director of Product Development at WiMetrics Corporation (WiMetrics), assignee of the above-identified U.S. patent application (the "patent application").

2. I have reviewed and understand the code modules listed in Exhibit A (supplied with the July 3, 2006, Office Action, another copy of which is attached hereto and also marked Exhibit A), which code modules existed prior to June 2002. As discussed more fully below, the pending claims of the patent application read on and cover these code modules.

3. Claim 1, as originally filed and as currently pending, reads as follows:

> A system for detecting and managing intrusion to a computer network from an unknown wireless device, the system comprising:
>
> a security component residing on the computer network that:
>
> passively monitors for network traffic received from an unknown wireless device;
>
> creates a device profile of the unknown wireless device;
>
> determines whether the unknown wireless device is an authorized device; and

> if the unknown wireless device is determined to be an authorized device, permits the network traffic from the unknown wireless device to pass to the computer network.

4. The software that result from building the code[1] listed in Exhibit A form, and/or are used on, "a ***system for detecting and managing intrusion to a computer network from an unknown wireless device***." This is a general description of the functionality of the code modules.

5. The code that results from building **FILTER.C** includes "a ***security component residing on the computer network.***" More specifically, **FILTER.C** is a component that when executed bridges communications from wireless devices to a computer network. This security component, generated from building the code of **FILTER.C**, connects to, or bridges, communications between two communication channels called "adapters," specifically <u>adapter0</u> and <u>adapter1</u>. As stated in the comments on page 2 of **FILTER.C**, <u>adapter0</u> is connected to a wireless access point. Similarly, as stated in the comments on page 5 of **FILTER.C**, <u>adapter1</u> is connected to the network backbone. Since a function of the **FILTER.C** component is to bridge communication from a valid wireless device to the network backbone, and since the **FILTER.C** component resides on the computer network (per its connection to <u>adapter1</u>), the **FILTER.C** component forms "***a security component residing on the computer network*** ."

6. The function "***passively monitors for network traffic received from an unknown wireless device***," is an operation of the security component of **FILTER.C**, as performed in the **ReceiveAdapater0()** routine. **ReceiveAdapater0()** begins on page 3 of Exhibit A. In this routine, a packet, <u>lpPacket</u>, is allocated, cleared, and initialized, after which passive monitoring

[1] "Building the code" is a common term used in software development to refer to a general process of converting source code to an executable form. This process includes compiling source code into object code and linking object code modules into executable code.

begins. Passive monitoring is conducted by way of calling the routine **PacketReceivePacket()**, with the parameters lpAdapter0, lpPacket, and TRUE. The routine **PacketReceivePacket()** is part of an open source network library that existed at the time and was used in conjunction with this system. The call to **PacketReceivePacket()** causes the security component to wait for a packet to arrive on the wireless network adapter, adapter0, (via the pointer lpAdapter0). Since the routine waits for a packet to arrive on adapter0, the call is passive, i.e., it passively waits/monitors for network traffic (a packet) from an unknown wireless device. When a packet is received, a call is then made to the routine **ExtractFrame_LANadapter0**. The source code for the routine **ExtractFrame_LANadapter0** is found on page 5. In **ExtractFrame_LANadapter0**, the security component extracts the wireless device MAC address from the packet and attempts to validate the MAC address, such that only valid devices are bridges (i.e., transferring the packed to adapter1 via the call to **Send_Adapater1**). Hence, the security component formed from the code **FILTER.C** "***passively monitors for network traffic received from an unknown wireless device.***"

7. The function "***creates a device profile of the unknown wireless device***," is an operation of the security component of **FILTER.C**, and is performed by the routine **validateMAC** as found on page 10. Creating a device profile for the unknown wireless device refers to information gleaned from a wireless device attempting to connect to the network, which device is current unknown to the system. As shown in **validateMAC**, the security component retrieves into memory the MAC address of an unknown wireless device from the Ethernet frame (pointed to by frame_start) sent by the unknown wireless device. The MAC address corresponds to a profile for the unknown wireless device. Further, as described in the comments to **validateMAC** as found on page 11, if the MAC address does not correspond to an authorized address in the Authorized table, the address is added to an UnAuthorized table. A MAC address

of an unknown and unauthorized device stored in an UnAuthorized table is a profile of the unknown device. Hence, the security component formed from the code **FILTER.C** "***creates a device profile of the unknown wireless device.***"

8. The function "***determines whether the unknown wireless device is an authorized device,***" is an operation of the security component of **FILTER.C**, and is also performed by the routine **validateMAC** as found on page 10. In the routine **ValidateMAC**, comparisons are made to determine whether or not the MAC address of the sender (of the Ethernet frame pointed to by frame_start) is in the Authorized table. In fact, the comments to the code explicitly state "// See if source MAC address in [sic] in the authorized table." Hence, the security component formed from the code **FILTER.C** determines "***whether the unknown wireless device is an authorized device.***"

9. The function "***if the unknown wireless device is determined to be an authorized device, permits the network traffic from the unknown wireless device to pass to the computer network,***" is an operation of the security component of **FILTER.C**, and is implemented, in part, in the routine **ExtractFrame_LANadapter0** (as found on page 5 in Exhibit A). A result corresponding to whether the wireless device is an authorized device (as described above) is returned from the routine **ValidateMAC** (as found on page 11). As shown in **ExtractFrame_LANadapter0**, if the value returned from **ValidateMAC** equals 1, the routine **ExtractFrame_LANadapter0** passes a pointer to the packet's frame, via the local variable base, to the computer network via the call to the routine **Send_Adapter1**. Passing the packet's Ethernet frame from the wireless device to the network constitutes "bridging" the communication from the wireless device to the computer network. Hence, the security component formed from the code **FILTER.C** performs the determination and results in "***if the unknown wireless device***

is determined to be an authorized device, permits the network traffic from the unknown wireless device to pass to the computer network."

10. As described above, each element of the system described in Claim 1 was found in and disclosed by the code modules derived from **FILTER.C**, of Exhibit A, which system was in experimental use prior to June 2002.

11. Independent Claim 18, as currently pending, reads as follows:

> A computer-implemented method for detecting intrusions to a computer network, comprising:
>
>> passively monitoring for network traffic received from an unknown wireless device, and upon detecting network traffic from the unknown wireless device:
>>
>>> creating a device profile of the unknown wireless device;
>>>
>>> determining whether the unknown wireless device is an authorized device; and
>>>
>>> if the unknown wireless device is determined to be an authorized device, permitting the network traffic from the unknown wireless device to pass to the computer network.

12. The software that results from building the code listed in Exhibit A implements "***a computer-implemented method for detecting intrusions to a computer network.***" This is a general description of the functionality of the method implemented by the code modules.

13. The step of "***passively monitoring for network traffic received from an unknown wireless device,***" is carried out by the executable modules formed from **FILTER.C**, as described in detail above in paragraph 6.

14. The function "***passively monitoring ..., and upon detecting network traffic from the unknown wireless device,***" recites that at least one subsequent action is made when network traffic is detected from an unknown wireless device. The recitations that follow identify the subsequent actions, and are found in Exhibit A as described below. Hence, the code module

FILTER.C recites, as part of a method, "***passively monitoring ..., and upon detecting network traffic from the unknown wireless device.***"

15. The step of "***creating a device profile of the unknown wireless device,***" is carried out by the executable modules formed from **FILTER.C**, as described in detail above in paragraph 7.

16. The step of "***determining whether the unknown wireless device is an authorized device,***" is carried out by the executable modules formed from **FILTER.C**, as described in detail above in paragraph 8.

17. The step of "***if the unknown wireless device is determined to be an authorized device, permitting the network traffic from the unknown wireless device to pass to the computer network,***" is carried out by the executable modules formed from **FILTER.C**, as described in detail above in paragraph 9.

18. As described above, each step of the method recited in Claim 18 is found and disclosed in the code modules derived from **FILTER.C**, of Exhibit A, which method was in experimental use prior to June 2002.

19. Independent Claim 34, as currently pending, reads as follows:

> A computer-readable medium having computer-executable instructions, which, when executed, carry out the method for detecting intrusions to a computer network, comprising:
>
> passively monitoring for network traffic received from an unknown wireless device, and upon detecting network traffic from the unknown wireless device:
>
> creating a device profile of the unknown wireless device;
>
> determining whether the unknown wireless device is an authorized device; and
>
> if the unknown wireless device is determined to be an authorized device, permitting the network traffic from the unknown wireless device to pass to the computer network.

20. Independent Claim 34 is directed to a computer-readable medium having computer-executable instructions which, when executed, carry out the method recited in independent Claim 18. It is well known that when a software product is built, the resultant code modules are placed in a computer-readable medium such that they can be executed. Typically, the computer-readable medium would include a hard disk drive, a CD-ROM, a floppy disk, or the like. Alternatively, the computer-readable medium may include computer memory, from which the computer-executable instructions may be executed. As building the code modules corresponding to **FILTER.C** creates computer-executable instructions stored in a computer-readable medium, and as the method carried out by these instructions is the same method as recited in independent Claim 18 (as discussed above in regard to paragraphs 11-18), the elements of independent Claim 34 are found and disclosed in the code modules derived from **FILTER.C**, of Exhibit A, and were in experimental use prior to June 2002.

21. All statements made herein are true, and all statements made on information and belief are believed to be true. These statements were made with the knowledge that willful, false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful, false statements may jeopardize the validity of the above-identified patent application or any patent that issues thereon.

Date: April 16, 2007

Jim Flanagan

OIPE
IAP41
APR 2 3 2007
PATENT & TRADEMARK OFFICE

MAIL STOP RCE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Joel Rosenberger	Attorney Docket No.: WIMET121663
Application No.:	10/669,124	Art Unit: 2131 / Confirmation No: 2882
Filed:	September 23, 2003	Examiner: Christopher A. Revak
Title:	SYSTEM AND METHOD FOR WIRELESS LOCAL AREA NETWORK MONITORING AND INTRUSION DETECTION	

TRANSMITTAL UNDER M.P.E.P. § 724
PROPRIETARY MATERIAL

Seattle, Washington 98101

April 20, 2007

TO THE COMMISSIONER FOR PATENTS:

The materials in the accompanying sealed envelope are considered proprietary and are being submitted to the United States Patent and Trademark Office for consideration under M.P.E.P. § 724.

Respectfully submitted,

CHRISTENSEN O'CONNOR
JOHNSON KINDNESS^PLLC

Tracy S. Powell
Registration No. 53,479
Direct Dial No. 206.695.1786

I hereby certify that this correspondence is being deposited with the U.S. Postal Service in a sealed envelope as first class mail with postage thereon fully prepaid and addressed to Mail Stop RCE, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the below date.

Date: April 20, 2007 Lori A Lewis

TSP:lal

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^PLLC
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100